Innovations for Port Security

Technologists and users must partner for success.

by Dr. Marc B. Mandler
Technical Director, U.S. Coast Guard Research and Development Center

Many of us have pondered the riddle about the tree that falls in the forest with nobody in earshot. Does the tree make a sound? In the spirit of this classic riddle, here is another puzzle: If an inventor creates a solution to a problem, but no one ever adopts the solution, is it considered an innovation?

Some argue that creativity is the mother of innovation. Therefore, a solution that is not embraced by end users should still be considered an innovation if it is novel and creative. In the corporate world, where generating profits is paramount, chief executive officers will say that products that do not generate or have the potential to generate profits, no matter how creative, should not be called innovations.

Acquirers of port security technologies view the world a little differently when it comes to innovations. They are inundated with information on hundreds, perhaps thousands, of technologies that are promoted as improving port security. Are all of these innovations? The acquirers of port security technologies—federal, state, and local officials—view innovations as not simply those products that have the promise of improving the security of a port, but products that are proven to improve security and do it in an affordable and cost-effective manner.

How does one create a better environment for innovation in port security? Significant funding has been made available through a variety of sources to address security needs. Sometimes, the funding is provided to technology developers to create products that can improve security posture. Other funds are provided to federal, state, or local authorities to acquire the best technology for a specific application. Technology developers are poised to provide the quick, off-the-shelf solution. Their customers search for the off-the-shelf system that will address their perceived vulnerability. The U.S. taxpayer trusts that officials will be good stewards of their tax dollars and protect them from many of the security risks that they currently face.

Dr. Robert Frosch, a former administrator of the National Aeronautics and Space Administration and former vice president of General Motors, provides some caution to developers and acquirers alike in an article, "The Customer for R&D is Always Wrong."[1] He writes:

"After 40-odd years of working in application- and mission-oriented research, I have come to believe profoundly that the customer for technology is always wrong. Now, the technologists are usually wrong, too; they tend to be wrong in complementary ways. I have seldom, if ever, met a customer for an application who correctly stated the problem to be solved. The normal statement of the problem is either too shallow and short-term, or, even more likely, is a formula for the widget that the customer thinks is required to solve what the customer thinks is the problem. The technologist is usually peddling 'that wonderful thing we did in the laboratory yesterday,' and if it happens to be square and the hole is round, a little force-fitting may help."

To overcome the wrongness that Dr. Frosh says permeates discussions between technologists and customers, there needs to be a robust and active collaboration between technology developers and technology consumers. Technology developers will be more successful if they walk in the shoes of the customer to gain a

full appreciation of the environment in which the user operates. Those constraints can prevent a technology solution from becoming an innovation.

Similarly, technology users must be willing to invite developers to work alongside them and teach them about their world and then be willing to have their operations serve as the testing ground for evaluating new technology concepts. Innovation is intimately related to the degree to which the technologist and user work together to clearly define the problem, the desired outcome, and the characteristics of a successful solution.

Modeling and Simulation as Innovation Tools

Modeling and simulation are tools that can help promote the innovation process and facilitate dialog between technologist and acquirer. Models or simulations provide an environment to test out technology concepts, in a relatively low-cost way before development funds are expended, to evaluate the effectiveness of potential technology solutions.

The Coast Guard Research and Development Center (RDC), the Coast Guard's sole research facility, uses many tools to assist in technology evaluations to support port security decisions. Simulation models are used to examine, for example, the relationship between surveillance system coverage and resolution and the likelihood of detecting a target of interest. Models are also used to evaluate the effectiveness and costs of employing, for example, small unmanned aerial vehicles in support of Coast Guard port security missions. In recent work, RDC used models to examine the effectiveness of waterside barriers for protecting vessels and facilities and different screening strategies for reducing the risk to ferries and passengers of a vehicle-borne improvised explosive device.

Consider a facility operator who wants to protect a facility, cruise ship, or a liquefied natural gas (LNG) tanker from attack by a small boat carrying explosives. Physical barriers, devices placed in the water to stop or slow down a small boat, offer promise for protection.

Figure 1: The new Hawkeye port surveillance system at Sector Command Center Miami.

RDC completed a study in partnership with the Captain of the Port in Boston, the city of Boston, and others to select the best commercial, off-the-shelf barrier to protect LNG ships moored in downtown Boston and cruise ships that make ports of call in Boston. The city of Boston was looking for stopping capability but was also concerned about mobility in its ports, the ease with which a barrier can be put in place and removed, and how much deterrence to an attack a barrier would provide without incurring excessive maintenance and support costs. A layer of protection analysis, which is a risk-based model, was used to evaluate the range of factors important to the port and to aid in selecting the barrier that fit the needs of the port. The result of this collaborative analysis was consensus among a number of disparate groups on the best set of technologies and operations to protect LNG vessels and cruise ships. The process of using a model to educate the consumer helps improve the likelihood that the technology selected will actually improve security.

Similarly, RDC worked closely with the ferry industry and federal, state, and local authorities to examine the range of alternatives that could be used to protect ferries from attack by a vehicle-borne improvised explosive device. A range of commercial vehicle screening technologies was examined, and a simulation model was developed to illustrate the trade-offs among screening effectiveness, cost, and efficiency of ferry operations. This effort, done in conjunction with authorities and ferry operators, resulted in recommendations that are being implemented to reduce the risk to the ferry system.

Rapid Prototyping Promotes Dialog with Users

Another powerful tool to promote the innovation process and facilitate a robust partnership between technologist and user is rapid prototyping. Rapid prototyping is an iterative process whereby a technology concept is matured through a spiral cycle of technology improvements that evolve from user feedback during the technology development process. Rapid prototyping is especially useful as a tool to help refine operational requirements in situations where users must adapt to a new mission or a new way of doing business.

Shortly after September 11, 2001, the Coast Guard Research and Development Center began a program called CATS-I that used this rapid prototyping process to improve the capabilities at the port level to prevent and respond to terrorist incidents. At the port level, operators understood their need to maintain situation awareness of the activities in and around the port, but they did not have enough experience in port security to articulate their operational requirements. Sectors Miami and San Francisco served as test beds for rapid prototyping of a variety of technologies, such as port surveillance systems, port partner collaboration tools, trip wires, and blue force tracking tools (technologies that tell units where friendly forces are).

RDC developed a robust collaborative relationship with other Coast Guard and port partners in Miami and San Francisco and worked closely with these partners to improve and refine the understanding of operational requirements. A significant accomplishment from this rapid prototyping effort was the development of rudimentary surveillance technologies, blue force tracking tools, and port partner collaboration tools that were demonstrated to improve the productivity and effectiveness at the sector.

The success of the CATS-I rapid prototyping process spurred the Department of Homeland Security Office of Science and Technology to make significant investments in the development of a full-scale, operational port-level surveillance and command and control system in Miami. This system, called Hawkeye (Figure 1), being developed by the Coast Guard's Command and Control Engineering Center, continues to serve as a test bed for experimentation for sector-level technology improvements. Sector Miami staff play a key role in providing feedback to developers on the capabilities and the effectiveness of the system design. Further, Hawkeye is serving as a basis for the Coast Guard's Command 2010 program, to refine requirements and evaluate new technology concepts for the Coast Guard acquisition of sector command center capabilities.

A partnership between technologist and technology acquirer/user is essential for improving port security. While some funding is flowing to ports to improve their security posture, ports are large, the vulnerabilities are significant, and the funding is limited. Everyone involved in securing ports has a responsibility to participate in the process of innovation, so that the best and most economical technologies can be found to secure U.S. ports. True innovation is realized when technologists and users work together to achieve common goals.

About the author: *Dr. Marc Mandler is technical director of the Coast Guard Research and Development Center in Groton, Conn. He received a B.A. in psychology from Clark University and a Ph.D. in psychology from University of Rochester. He has been a civilian employee of the Coast Guard for more than 22 years.*

Endnote

[1] Research Technology Management, November-December 1996, pp 22-27.